CLAIMS

What is claimed is:

1. An apparatus to manage a plurality of device configurations comprising:

a control server to generate a job to update a device;

a control point to establish a secure communication with the control server, and to receive the job;

the control point to establish communication with the device in accordance with a maintenance schedule, and to update the device using the job.

2. The apparatus of claim 1, wherein the control server and the control point are co-resident on a single computer system.

3. The apparatus of claim 1, wherein the control point is further to communicate a result of the update process to the control server.

4. The apparatus of claim 3, wherein the communication of the result of the update process comprises a transcript of communication between the device and the control point.

5. The apparatus of claim 1, further comprising:

a data store coupled to the control server, the data store including a device profile identifying the device to be updated and the device's characteristics.

6. The apparatus of claim 5, wherein the control server comprises:

a data generator to generate device specific data from the device profile; and

a template interpreter to generate the job script based on the device specific data and template data.

7. The apparatus of claim 6, wherein a template group is attached to the device profile.

8. The apparatus of claim 6, wherein each device profile includes a device type, and a template group is attached to each device type.

9. The apparatus of claim 6, wherein the template interpreter further points to configuration files and supporting files.

10. The apparatus of claim 9, wherein the control point uses the job to interact with the device, and uploads the configuration files to the device.

11. The apparatus of claim 1, wherein the job is to audit the device.

12. The apparatus of claim 11, wherein the audit comprises retrieving configuration files from the device.

13. The apparatus of claim 11, wherein the audit comprises retrieving firmware from the device.

14. The apparatus of claim 11, wherein the audit comprises obtaining a checksum of the firmware of the device

15. The apparatus of claim 1, wherein the control server generates a job in response to receiving a change in the device profile.

16. The apparatus of claim 15, wherein the change in the device profile is made using a command line interface.

17. The apparatus of claim 1, wherein the control server further comprises a control point generator to permit creation of a new control point.

18. The apparatus of claim 17, wherein the control point generator comprises:

a localizer to generate a localized control point executable;

wherein the localization identifies a control server, such that the control point executable may only interface with the identified control server.

19. The apparatus of claim 18, wherein the identified control server is a control server group.

20. The apparatus of claim 19, wherein a single control server is designated as a default control server, and other members of the control server group enable fail-over if the default control server is unavailable.

21. The apparatus of claim 18, wherein the localized control point executable includes the control server's public key.

22. The apparatus of claim 17, wherein the control point generator comprises:

a pass phrase generator to generate a one-time pass phrase;

wherein upon installing a localized control point executable, the localized control point executable is activated using the pass phrase.

23. The apparatus of claim 22, wherein the pass phrase is a series of words from a dictionary.

24. The apparatus of claim 23, wherein pass phrase encodes a one-time password.

25. The apparatus of claim 17, wherein when the new control point is initialized using the localized control point executable, the new control point comprises:

a key generation logic to generate a public key and a private key for the control point;

a secure communication mechanism to communicate with the control server using a one-time password encoded in a pass phrase used to generate the new control point; and the secure communication mechanism to complete a key exchange with the control server, such that public key cryptography is used for further secure communication.

26. The apparatus of claim 1, further comprising:

a scheduler in the control server to schedule an update of a particular device coupled to a control point, and when it is time to update the particular device, to send a communication request to the control point; and

a secure communication mechanism in the control point to respond to the request by establishing a secure communication link with the control server.

27. The apparatus of claim 26, wherein the secure communication link is secure shell (SSH).

28. The apparatus of claim 26, wherein the secure communication link is secure sockets layer (SSL).

29. The apparatus of claim 26, wherein the time to schedule an update of a particular device corresponds to a maintenance window of the device.

30. The apparatus of claim 26, wherein the device being updated is the control point.

31. The apparatus of claim 1, wherein the control point further comprises:

a scheduler to schedule execution of each job received by the control point; and

a reporter to report back results of the execution of each job to the control server.

32. The apparatus of claim 31, wherein the results comprise a complete transcript of communication with the device to which the job was directed.

33. The apparatus of claim 1, further comprising a data store including a device profile defining a current state of the device.

34. The apparatus of claim 33, wherein the data store is a SQL database, and the data store is displayed as a hierarchical data store.

35. The apparatus of claim 33, wherein the data store comprises a plurality of data types and new data types may be arbitrarily defined.

36. The apparatus of claim 33, wherein the data store further comprises the past states of the device.

37. The apparatus of claim 34, further comprising a service module coupled to the control server, the service module to define a functionality that may be provided through the control server, the service module having a separate user interface.

38. The apparatus of claim 37, wherein a service module comprises:

a user interface;

a command line interface to receive user input and convert it into commands; and

a service module core to define a functionality to alter data in the data store, such that the change flows down to the control points and the devices.

39. The apparatus of claim 38, wherein the service module core is further to define arbitrary attributes for data in the data store.

40. A control server to manage a plurality of device configurations comprising:

a data store to store current status of each device;

a user interface to alter data in the data store to prompt creation of a job;

a scheduler to schedule jobs to update devices;

a control point interface to send jobs to a control point, and to receive a result from the control point.

41. The control server of claim 40, wherein the user interface is a command line interface (CLI) permitting the creation of action scripts to make complex alterations to the devices, the control points, and the data store.

42. The control server of claim 40, wherein the data store is an SQL database presented in a hierarchical fashion.

43. The control server of claim 40, further comprising a device module to generate a job for a particular device.

44. The control server of claim 43, wherein the device module comprises:

a controller to create data from a device profile; and

a master to create a job using the data produced by the controller.

45. The control server of claim 44, wherein the master further to determine whether to create a job.

46. The control server of claim 44, wherein the device module further comprises:

a template to create device configuration files; and

a job to deliver changes to the device.

47. The control server of claim 44, wherein the device profile comprises a descriptive triplet including a device module name, device platform, and firmware revision, the device profile specifying how a particular device is configured.

48. A control point to serve as an interface to a plurality of devices, the control point managed by a control server, the control point comprising:

a scheduling logic to schedule a job in accordance with a maintenance window defined by the job;

an execution environment for a delivery driver to deliver a job to a device in accordance with the maintenance window of the device, as specified by the job.

49. The control point of claim 48, further comprising:

the scheduling logic to schedule interfacing the control point with the control server to receive jobs and updates.

50. The control point of claim 48, further comprising:

a secure communications channel to securely communicate with a control server.

51. The control point of claim 48, wherein the control point is a stand-alone system, running a secure/hardened operating system.

52. The control point of claim 48, wherein the control point operates as an application on a non-dedicated computer system.

53. The control point of claim 52, wherein the control point on the non-dedicated computer system further comprises:

a system state monitor to control the network and network applications settings on the standard computer system.

54. The control point of claim 48 further comprising:

a cache to store files used by a job, such that the files may be reused and the jobs sent need not include the files.

55. The control point of claim 54, a wherein a job includes references to a plurality of files, and if the files are not in the cache, the secure communications channel further to request the files from the control server.

56. The control point of claim 48, further comprising:

an execution environment for delivery drivers to execute the indicated processes and jobs.

57. The control point of claim 48, wherein the control point has a maintenance window, such that the control point is updateable by the control server.

58. A method of controlling a network comprising:

determining if there is a job for a control point;

establishing a secure connection between a control server and the control point;

sending the job to the control point, including a maintenance window during which the job is to be performed; and

receiving job statuses of previous jobs from the control point; and

closing the connection with the control point.

59. The method of claim 58, wherein the job is to update the control point, and the maintenance window is the maintenance window of the control point.

60. The method of claim 58, wherein the job is to update a device coupled to the control point.

61. The method of claim 58, wherein if the job is to update a device coupled to the control point, the maintenance window is the maintenance window of the device to which the job applies.

62. A method of controlling a network comprising:

establishing a secure session between a control server and a control point;

receiving a job from the control server, including a maintenance window during which the job is to be performed;

putting the job into a job queue;

sending job statuses of previous jobs to the control server; and

closing the connection with the control server.

63. The method of claim 62, further comprising:

determining that there is a job in the job queue that has a current maintenance window;

connecting to the device using credentials;

executing the job in the control point to affect the device;

storing the results of the job as the job status; and disconnecting from the device.

64. The method of claim 63, wherein the credentials are a password.

65. The method of claim 63, wherein running the job comprises:

determining if the device is in an expected state; and

updating and configuring the device as specified by a job script within the job.

66. The method of claim 63, wherein if the device is not in the expected state, the device is not updated, and the non-compliant state data is returned to the control server.

67. The method of claim 66, further comprising:

raising an alarm when the non-compliant state data is returned.

68. A method of controlling a network including a control point controlled by a control server, the control point controlling the devices on the network in accordance with jobs sent by the control server, the method including creating new control points, the method of creating a control point comprising:

generating a branded executable for the control point including the control server's public key;

generating a passphrase including a one-time password for activating the control point; and upon installation of the branded executable and activation with the passphrase, receiving a connection from the new control point using the one-time password from the passphrase.

69. The method of claim 68, further comprising:

verifying that the control point identified by the one-time password is valid and not yet activated; and

establishing a secure communications channel with the control point.

70. The method of claim 68, wherein the passphrase is a plurality of words in the English language.

71. The method of claim 68, wherein the passphrase is three or more words having four or more letters, such that the passphrase is easily transmitted via voice communication.

72. The method of claim 68, further comprising:

creating a public/private keypair for the new control point, and using that public/private keypair for establishing secure communication with the control point.

73. A method of controlling a network using a control server, the method comprising:

maintaining a data store including configurations of each device coupled to the control server through a control point;

generating a job to update a device;

receiving a report from the control point regarding the execution of the job to update the device; and

storing in the data store the report with the current configuration of the device, such that a complete revision history of the device is maintained.

74. The method of claim 73, wherein the revision history of the device includes a previous device profile for that device, enabling a new device to be configured identically to the original device, even if the new device is of a different make.

75. The method of claim 73, wherein the revision history of the device includes a previous device configuration file, enabling a review of the state of the device at any point in the past.

76. The method of claim 73, wherein the revision history includes time and date stamps for each alteration to a device.

77. The method of claim 73, wherein the job is generated in response to a change in the data store.

78. A method of controlling a network including a control point controlled by a control server, the control point interacting with the devices on the network in accordance with jobs sent by the control server, the method comprising generating a job comprising:

identifying a device profile of the device for which the job is to be generated;

using a controller in the device profile to preprocess data needed for the job; and

using a master in the device profile to generate the job based on the preprocessed data, thereby creating a job for the device.

79. The method of claim 78, further comprising:

the master determining that no job needs to be generated.

80. The method of claim 78, wherein the job is generated in response to a change in a data store.

81. The method of claim 78, wherein the job includes a maintenance window of the device, the maintenance window defining a time period during which the job is to be executed.

82. The method of claim 78, wherein the job includes a JobScript to execute the job.

83. The method of claim 78, wherein the job references other data in a data store, used by the job.

84. The method of claim 83, wherein if the other data is already in a cache in the control point, it is not sent to the control point.

85. A method of remotely manipulating a device coupled to a control point, the control point managed by a control server, comprising:

generating a job to manipulate the device;

sending the job to the control point to which the device is coupled; and

providing an execution engine to execute the job on the control point.

86. The method of claim 85, wherein manipulating the device comprises one or more of the following: initializing the device, updating the device, configuring the device, and auditing the device.